Юридические исследования
Правильная ссылка на статью:
Новиков П.А. Современные вызовы в обеспечении защиты персональных данных работников // Юридические исследования. 2025. № 3. DOI: 10.25136/2409-7136.2025.3.73694 EDN: YKSZHR URL: https://nbpublish.com/library_read_article.php?id=73694

Современные вызовы в обеспечении защиты персональных данных работников

Новиков Петр Александрович

ORCID: 0009-0009-5133-811X

аспирант; ЧОУ ВО "Санкт-Петербургский университет технологий управления и экономики"

190020, Россия, г. Санкт-Петербург, Лермонтовский пр-т, д.44, Лит.А

petnovikov.81@mail.ru

Статья из рубрики "Человек и государство"

DOI:

10.25136/2409-7136.2025.3.73694

EDN:

YKSZHR

Дата направления статьи в редакцию:

14-03-2025

Аннотация: В эпоху цифровой трансформации, когда данные стали неотъемлемой частью бизнес-процессов, вопрос защиты персональных данных работников приобретает первостепенное значение. Современные организации сталкиваются с беспрецедентными вызовами, связанными с необходимостью соблюдения нормативных требований, противодействия киберугрозам и поддержания доверия работников. Данное исследование направлено на анализ этих вызовов и выработку практических рекомендаций для эффективного обеспечения защиты персональных данных работников. Обеспечение защиты персональных данных работников является сложной и многогранной задачей, требующей от организаций комплексного подхода и постоянного совершенствования своих политик и процедур. Соблюдение требований законодательства, противодействие киберугрозам, обеспечение прозрачности и контроля за обработкой данных, а также учет специфики отдельных категорий персональных данных являются ключевыми факторами успеха в этой области. Методологической основой исследования является комплексный подход, сочетающий в себе анализ нормативно-правовой базы и экспертные оценки. Одним из ключевых

аспектов научной новизны является выявление и систематизация новых угроз безопасности персональных данных, обусловленных использованием современных технологий. К таким угрозам относятся, в частности, утечки данных, вызванные кибератаками на информационные системы работодателя, неправомерный доступ к персональным данным со стороны инсайдеров, а также риски, связанные с использованием облачных сервисов и мобильных устройств для обработки и хранения персональной информации. Другим важным элементом научной новизны данного исследования является разработка методологии оценки эффективности существующих мер защиты персональных данных работников. Традиционные методы оценки, как правило, ориентированы на общие требования законодательства о защите персональных данных и не учитывают специфические риски, возникающие в контексте трудовых отношений.

Ключевые слова:

персональные данные, обработка данных, права работников, комплаенс, облачные технологии, искусственный интеллект, интернет вещей, кибербезопасность, утечки данных, политика конфиденциальности

Введение

В условиях стремительного развития информационных технологий, глобальной цифровизации и широкомасштабного внедрения электронных систем хранения и обработки данных вопросы защиты персональных данных приобретают особую значимость. Современное общество, основанное на принципах технологической взаимосвязанности и оперативного обмена информацией, сталкивается с растущими рисками несанкционированного доступа к конфиденциальной информации, неправомерного использования персональных данных, их утечки, модификации и уничтожения вследствие кибератак, технических сбоев или действий третьих лиц. Эти угрозы затрагивают как физических лиц, так и юридических субъектов, ведущих деятельность в различных сферах экономики и общественных отношений. В особенности указанная проблема касается персональных данных работников, обрабатываемых работодателями в ходе исполнения трудовых отношений и кадрового администрирования. Такие данные включают сведения о личности работников, их профессиональной деятельности, медицинских показателях, финансовом положении и иных аспектах, что делает их объектами повышенного внимания со стороны злоумышленников и требует надежной правовой и технической защиты на всех этапах их жизненного цикла.

Государственное регулирование защиты персональных данных направлено на создание унифицированных стандартов информационной безопасности, правовое урегулирование процессов обработки данных и обеспечение эффективного механизма гражданско-правовой защиты интересов субъектов персональных данных [1]. В Российской Федерации основным нормативно-правовым актом, регулирующим отношения в данной сфере, является Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», который определяет основные принципы, правовые основания и требования к обработке, хранению, передаче и уничтожению персональных данных. Данный закон закрепляет права субъектов персональных данных, устанавливает обязанности операторов по их обработке, предусматривает меры защиты информации и ответственность за допущенные правонарушения. Однако практика его применения

демонстрирует наличие значительных трудностей, обусловленных как техническими и организационными аспектами, так и пробелами, и коллизиями в правовом регулировании. В условиях активного внедрения новых цифровых технологий, таких как искусственный интеллект, облачные вычисления, распределённые реестры (блокчейн), Интернет вещей, технологии анализа больших данных (Big Data) и биометрические идентификационные системы, традиционные механизмы защиты информации сталкиваются с новыми вызовами, требующими адаптации нормативно-правовой базы, разработки и внедрения комплексных технических решений и совершенствования методов правоприменения.

Среди наиболее значимых проблем в сфере защиты персональных данных работников можно выделить несколько ключевых направлений. Во-первых, технологические риски, связанные с уязвимостью программного обеспечения, недостаточной защищённостью информационных систем и угрозой кибератак. В современном мире обработка персональных данных осуществляется с применением цифровых платформ, облачных хранилищ, мобильных приложений и автоматизированных систем документооборота, что существенно расширяет потенциальные векторы атак на персональную информацию и требует совершенствования мер информационной безопасности, шифрования и защиты данных от несанкционированного доступа. Во-вторых, правовые коллизии, возникающие в связи с противоречиями между национальными и международными нормами, сложностями в определении юрисдикции при трансграничной передаче данных и отсутствием четких регламентов взаимодействия между операторами и уполномоченными органами. В-третьих, организационные трудности, связанные с необходимостью обеспечения должного уровня защиты информации в компаниях, отсутствием единых стандартов корпоративной политики в области кибербезопасности, а также недостаточной осведомлённостью работников о мерах защиты персональных данных. В-четвёртых, этические вопросы, касающиеся баланса между правых работников на защиту их частной жизни и интересами работодателей, связанными с необходимостью контроля за деятельностью работников, мониторингом их рабочей активности, использованием биометрических данных и иных способов идентификации [2].

Эффективное решение вышеуказанных проблем требует детального анализа действующего законодательства, практики его применения, международного опыта регулирования обработки персональных данных, а также разработки и внедрения комплексных механизмов гражданско-правовой защиты прав субъектов персональных данных. Важную роль в этом процессе играет формирование корпоративной культуры в области кибербезопасности, разработка и внедрение внутренних регламентов обработки персональных данных, соответствующих международным стандартам, таким как Общий регламент защиты данных (GDPR) Европейского союза, а также нормативным актам Совета Европы и ООН[3]. Значительное внимание должно уделяться совершенствованию механизмов идентификации и аутентификации пользователей, внедрению передовых технологий защиты информации, таких как многофакторная аутентификация, биометрические системы доступа, использование блокчейн-технологий для обеспечения прозрачности обработки данных, а также методам машинного обучения для выявления аномалий и потенциальных угроз в информационных системах.

Таким образом, изучение вопросов гражданско-правовой защиты персональных данных работников в условиях цифровой трансформации представляет собой актуальную научно-практическую задачу, требующую всестороннего подхода, комплексного анализа и поиска эффективных правовых, организационных и технических решений. Данная статья направлена на исследование существующих проблем в области защиты

персональных данных, выявление правовых и технологических рисков, а также разработку предложений по совершенствованию гражданско-правового механизма защиты средств индивидуализации граждан (физических лиц) и их персональных данных, что позволит повысить уровень информационной безопасности в современной правовой и деловой среде.

Методология исследования строится на комплексном подходе, объединяющем анализ нормативно-правовой базы и экспертные оценки. Такой подход обусловлен необходимостью всестороннего изучения проблемы, учитывая как юридические аспекты, так и практические реалии функционирования систем обработки персональных данных в организациях.

Первым этапом является анализ нормативно-правовой базы, регулирующей защиту персональных данных. Анализ предполагает выявление пробелов, противоречий и неясностей в действующем законодательстве, которые могут создавать трудности в обеспечении защиты персональных данных работников.

Вторым этапом является проведение экспертных оценок. Цель данного этапа – выявить практические проблемы, возникающие при реализации требований законодательства о персональных данных, а также оценить эффективность существующих мер защиты персональных данных.

Сочетание анализа нормативно-правовой базы и экспертных оценок позволяет сформировать комплексное представление о современных вызовах в обеспечении защиты персональных данных работников, а также разработать практические рекомендации по совершенствованию системы защиты персональных данных в организациях.

Современные вызовы и технологические риски в области защиты персональных данных

Цифровая трансформация бизнеса привела к значительному увеличению объемов обрабатываемых персональных данных. Компании все чаще используют облачные хранилища, системы управления данными, платформы для обработки больших данных и искусственный интеллект для анализа информации. По мнению Д.А. Карташова такие инновации влекут за собой значительные угрозы для безопасности персональных данных работников, клиентов и партнеров. В условиях активного использования цифровых технологий возрастают риски утечки данных, неправомерного их использования и нарушения прав субъектов персональных данных. Современные вызовы требуют комплексного подхода к обеспечению информационной безопасности, учитывающего не только технические, но и правовые, организационные и поведенческие аспекты [4].

Одной из ключевых угроз являются кибератаки, направленные на несанкционированный доступ к базам данных, содержащим персональную информацию. Хакеры применяют различные методы атак, включая фишинг, вредоносное программное обеспечение, атаки через уязвимости в программном обеспечении и целенаправленные атаки на корпоративную инфраструктуру. Например, фишинговые атаки направлены на обман работников с целью получения доступа к конфиденциальной информации, а вредоносные программы могут шифровать файлы или красть данные. Известны случаи, когда крупные компании подвергались подобным атакам, что приводило к утечке данных миллионов пользователей. Например, утечка данных в результате взлома компании Yahoo в 2013 году затронула около трех миллиардов учетных записей пользователей. Также можно

привести пример взлома Equifax в 2017 году, когда злоумышленники получили доступ к персональным данным более 147 миллионов человек, включая номера социального страхования и кредитную информацию [5].

Д. Рымашевская считает, что использование Интернета вещей (IoT) в корпоративной среде также создает новые угрозы. Умные устройства, биометрические системы, камеры наблюдения и другие сенсоры могут стать объектами хакерских атак, если не обеспечена их надлежащая защита. Нередко утечки данных происходят из-за низкого уровня безопасности IoT-устройств, недостатка шифрования и слабых паролей [6]. Согласно исследованию О.В. Бычкова, около 70% IoT-устройств имеют критические уязвимости, которые могут быть использованы злоумышленниками [7]. В частности, в 2020 году были зафиксированы массовые атаки на системы видеонаблюдения, в ходе которых хакеры получили доступ к тысячам камер наблюдения, установленных в офисах, больницах и школах [8].

Удаленная работа и использование облачных технологий также увеличивают уязвимость систем. Многие компании перешли на гибридные и удаленные модели работы, что привело к увеличению числа устройств, подключенных к корпоративным сетям из различных местоположений. Это создает дополнительные точки уязвимости, если не используются надежные системы защиты, такие как VPN, многофакторная аутентификация и мониторинг аномальной активности. В соответствии с Федеральным законом Российской Федерации «О персональных данных» № 152-ФЗ, операторы персональных данных обязаны принимать меры по защите информации, включая организационные и технические меры безопасности. Однако, А.А. Миняев считает, что даже при соблюдении всех нормативных требований остаются риски, связанные с человеческим фактором и недостаточной цифровой грамотностью пользователей [9].

Г.А. Майстренко, рассматривая источники правового регулирования защиты персональных данных работника в России, считает, что социальная инженерия остается одним из наиболее опасных методов атаки. Даже самые современные системы безопасности могут оказаться бессильными перед человеческим фактором. Использование слабых паролей, неосторожное обращение с конфиденциальной информацией и отсутствие киберграмотности могут стать причиной серьезных утечек данных. Согласно отчетам по кибербезопасности, более 80% взломов происходят из-за использования слабых паролей или кражи учетных данных через методы социальной инженерии. Например, в 2020 году работники Twitter стали жертвами атаки социальной инженерии, в результате которой злоумышленники получили доступ к учетным записям известных личностей, включая Барака Обаму и Илона Маска [10].

Для минимизации рисков компаниям необходимо внедрять комплексные системы защиты, включающие шифрование данных, использование многофакторной аутентификации, постоянный мониторинг угроз и анализ поведения пользователей, регулярное обновление программного обеспечения и контроль доступа. Например, применение стандарта шифрования AES-256 позволяет существенно повысить уровень защиты данных. Кроме того, необходимо использовать технологии анализа аномалий поведения пользователей, которые могут выявлять подозрительные действия и автоматически блокировать потенциальные угрозы [11].

Важным аспектом защиты информации является также обучение персонала и повышение уровня киберграмотности работников. Согласно статье 19 Федерального закона № 152-ФЗ, операторы персональных данных обязаны обеспечивать безопасность персональной

информации, включая обучение работников методам защиты данных. Программы обучения должны включать тренинги по кибербезопасности, симуляцию фишинговых атак и регулярные проверки на знание политик безопасности. Например, крупные международные компании, такие как Google и Microsoft, проводят регулярные киберучения, направленные на повышение осведомленности работников о киберугрозах [12].

Также следует учитывать правовые аспекты защиты персональных данных. Например, в рамках европейского законодательства действует Общий регламент по защите данных (GDPR), который устанавливает строгие требования к обработке персональной информации. В случае нарушения норм GDPR компании могут быть оштрафованы на суммы до 20 миллионов евро или 4% от их годового оборота. В России аналогичные меры предусмотрены в Федеральном законе № 152-ФЗ, однако практика применения штрафных санкций пока не столь обширна [13].

Таким образом, защита персональных данных в условиях цифровой трансформации требует комплексного подхода, включающего как технические, так и организационные меры. Внедрение надежных систем безопасности, использование современных технологий защиты, а также повышение уровня киберосведомленности персонала являются ключевыми факторами в обеспечении информационной безопасности. При этом соблюдение норм действующего законодательства, таких как Федеральный закон «О персональных данных», является обязательным требованием для всех организаций, работающих с персональными данными. В будущем можно ожидать ужесточения регулирования в данной сфере, что потребует от компаний дополнительных инвестиций в информационную безопасность и внедрения новых технологий защиты данных.

Правовое регулирование и организационные меры защиты персональных данных

Соблюдение требований законодательства, по мнению О.К. Коробковой, является ключевым аспектом защиты персональных данных работников, поскольку информация о физических лицах требует надежной охраны от несанкционированного доступа, утечек и неправомерного использования. В Российской Федерации действует ряд нормативных актов, регулирующих данный вопрос, включая Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Трудовой кодекс Российской Федерации, а также многочисленные подзаконные нормативные акты, разрабатываемые Роскомнадзором и иными уполномоченными органами [14].

Согласно положениям Закона о персональных данных, компании обязаны получать осознанное согласие работников на обработку их персональных данных, за исключением случаев, предусмотренных законодательством. Также необходимо строго обосновывать цели обработки, ограничивать сроки хранения информации и применять адекватные меры защиты, включая шифрование, аутентификацию, управление доступом и аудит безопасности.

Одной из важных гарантий прав граждан является принцип минимизации данных, согласно которому работодатель должен запрашивать только те сведения, которые необходимы для выполнения законных обязанностей перед работником. В противном случае компания рискует столкнуться с административной ответственностью, предусмотренной ст. 13.11 Кодекса Российской Федерации об административных правонарушениях, за незаконное получение и обработку персональных данных.

Однако правоприменительная практика показывает, что многие организации

сталкиваются с трудностями в обеспечении выполнения данных норм. Среди основных проблем можно выделить отсутствие унифицированного стандарта обработки персональных данных в различных отраслях экономики, разночтения в интерпретации законодательства, а также сложность его адаптации к современным условиям цифровизации. Кроме того, недостаточный уровень информированности работников о своих правах и обязанностях в области защиты персональных данных также усугубляет проблему [15].

Так, например, в банковском секторе применяется один подход к обработке персональных данных клиентов и работников, включающий многоуровневые системы защиты, строгий контроль доступа и регулярный мониторинг информационных потоков. В то же время в малом бизнесе или в образовательных учреждениях защита персональных данных зачастую носит менее структурированный характер, что создает предпосылки для нарушения законодательства.

Еще одной сложностью является несоответствие внутренних регламентов компаний актуальным требованиям законодательства, что может привести к проверкам со стороны Роскомнадзора и наложению штрафов. Например, в 2023 году Роскомнадзор оштрафовал ряд крупных российских компаний за несоблюдение требований о хранении и обработке персональных данных, поскольку в их внутренних политиках отсутствовали положения о порядке удаления информации по истечении сроков хранения [16].

Для эффективного выполнения требований законодательства компаниям необходимо внедрять внутренние регламенты и политики по защите информации. Разработка локальных нормативных актов должна учитывать следующие ключевые аспекты [17]:

1. Определение порядка обработки персональных данных. В документе необходимо четко регламентировать категории обрабатываемых данных, цели их использования, сроки хранения и меры по их уничтожению после завершения необходимости обработки.

2. Меры защиты информации. Организация должна внедрять технические и организационные меры, такие как шифрование, резервное копирование данных, разграничение доступа, ведение журналов аудита и регулярное тестирование информационных систем на предмет уязвимостей.

3. Обязанности работников. Все работники должны быть ознакомлены с внутренними политиками защиты данных, проходить соответствующее обучение и нести ответственность за нарушение правил обработки персональной информации.

4. Механизмы контроля и ответственности. Работодатель обязан обеспечить контроль за соблюдением требований законодательства путем проведения регулярных внутренних аудитов, проверки логов доступа и ведения реестра инцидентов безопасности.

Также одним из эффективных методов повышения уровня защиты персональных данных является разработка методологии оценки эффективности существующих мер защиты персональных данных работников.

Разработка методологии оценки эффективности существующих мер защиты персональных данных работников представляет собой многоаспектную задачу, требующую комплексного подхода, основанного на нормативных требованиях, передовых практиках и специфике деятельности организации. Целью данной методологии является предоставление структурированного и измеримого способа оценки адекватности и результативности применяемых мер, направленных на обеспечение конфиденциальности,

целостности и доступности персональных данных работников.

Основой для разработки методологии служат положения Федерального закона №152-ФЗ «О персональных данных», который устанавливает общие требования к обработке персональных данных, включая принципы, условия и порядок осуществления такой обработки (Статья 5 Закона). Кроме того, учитываются положения иных нормативных актов, в том числе, Трудового кодекса Российской Федерации, определяющего права и обязанности работодателя и работника в части обработки персональных данных, а также подзаконных актов, регулирующих вопросы защиты информации [18].

Предлагаемая методология оценки эффективности включает следующие ключевые этапы (рис. 1):

Рис. 1 – Этапы оценки эффективности уровня защиты персональных данных работников

На первом этапе проводится детальный анализ процессов обработки персональных данных работников в организации. Определяются все категории персональных данных, включая идентификационные данные, контактные данные, сведения об образовании, трудовой деятельности, финансовые данные и другие. Важно отметить, что объем обрабатываемых данных должен быть строго ограничен целью обработки (Статья 5 Закона).

Второй этап предполагает выявление и анализ потенциальных угроз и уязвимостей, которые могут привести к неправомерной обработке, утечке, уничтожению или изменению персональных данных. Оценка рисков проводится с учетом вероятности наступления негативных последствий и степени ущерба, который может быть причинен субъектам персональных данных. В качестве отправной точки могут быть использованы методические рекомендации ФСТЭК России по оценке угроз безопасности информации.

На третьем этапе проводится детальное изучение применяемых организационных и технических мер защиты персональных данных. К организационным мерам относятся разработка и внедрение внутренних политик и процедур, регламентирующих порядок обработки персональных данных, обучение персонала, назначение ответственных лиц. К техническим мерам относятся использование средств защиты информации, таких как системы контроля доступа, шифрование, антивирусная защита, системы обнаружения вторжений и другие (Приказ ФСТЭК России №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных").

Четвертый этап предполагает оценку эффективности применяемых мер необходимо установить четкие и измеримые критерии. Критерии могут быть количественными

(например, количество инцидентов, связанных с нарушением конфиденциальности персональных данных, время восстановления после инцидента) и качественными (например, уровень осведомленности персонала о требованиях законодательства в области защиты персональных данных, степень соответствия применяемых мер требованиям нормативных актов).

На пятом этапе проводится оценка соответствия применяемых мер защиты установленным критериям эффективности. Оценка может проводиться путем проведения аудитов, тестирований на проникновение, анализа журналов событий, опросов персонала и других методов. Результаты оценки оформляются в виде отчета, содержащего выводы о степени эффективности применяемых мер и рекомендации по их совершенствованию.

На основании результатов оценки в ходе шестого этапа разрабатывается план мероприятий, направленный на устранение выявленных недостатков и повышение эффективности применяемых мер защиты. План мероприятий должен содержать конкретные действия, сроки их выполнения и ответственных лиц.

Важным аспектом методологии является обеспечение непрерывности процесса оценки эффективности мер защиты персональных данных. Оценка должна проводиться на регулярной основе, а также при изменении нормативных требований, технологической инфраструктуры или процессов обработки персональных данных. Результаты оценки должны использоваться для постоянного совершенствования системы защиты персональных данных в организации [19].

Дополнительно, для снижения вероятности несанкционированного использования персональных данных важно внедрение систем мониторинга доступа, автоматизированных средств защиты и инструментов аутентификации, таких как двухфакторная идентификация (2FA). В качестве примера можно привести практику ряда российских IT-компаний, которые используют строгую политику контроля доступа к данным, применяют систему биометрической идентификации и ведут централизованный учет всех действий с конфиденциальной информацией.

Немаловажным аспектом остается баланс между контролем работодателя и доверием к работникам. Избыточный контроль может привести к снижению уровня доверия внутри коллектива и ухудшению психологического климата в организации. Поэтому меры по обеспечению защиты персональных данных должны носить разумный и обоснованный характер, соответствующий принципу соразмерности, закрепленному в законодательстве о персональных данных [20].

Таким образом, эффективная защита персональных данных требует комплексного подхода, включающего не только выполнение законодательных норм, но и внедрение современных технологий защиты информации, повышение уровня правовой грамотности работников и создание культуры осознания важности защиты данных в корпоративной среде. Соблюдение этих принципов позволит минимизировать риски нарушения законодательства, избежать значительных штрафов и обеспечить надежную защиту персональных данных работников и клиентов компании.

Заключение

Защита персональных данных работников является многогранной и комплексной задачей, требующей скоординированных действий в технологической, правовой и организационной сферах. В условиях стремительного развития цифровых технологий и

процессов цифровой трансформации бизнеса компании сталкиваются с растущими вызовами, связанными с обеспечением информационной безопасности. Угрозы, такие как утечки конфиденциальной информации, несанкционированный доступ, кибератаки, вредоносное программное обеспечение и социальная инженерия, становятся все более распространенными и сложными.

Одним из ключевых аспектов защиты персональных данных является совершенствование нормативно-правового регулирования, устанавливающего требования к обработке, хранению и передаче информации. В современных условиях необходимо учитывать, как национальное законодательство, так и международные стандарты в области защиты данных, такие как Общий регламент по защите данных (GDPR), Конвенция 108+ Совета Европы и другие нормативные акты. Внедрение строгих стандартов безопасности позволяет повысить уровень правовой защиты работников и снизить вероятность нарушений, связанных с обработкой их персональных данных.

Не менее важным направлением является использование современных технологических решений, обеспечивающих высокий уровень защиты информации. Среди таких решений можно выделить системы шифрования данных, средства контроля доступа, биометрическую аутентификацию, инструменты мониторинга активности пользователей, системы предотвращения утечек данных (DLP) и средства защиты от вредоносных программ. Применение передовых технологий способствует минимизации рисков несанкционированного распространения персональной информации и повышает общий уровень кибербезопасности в организации.

Однако технологические меры сами по себе не могут гарантировать абсолютную защиту персональных данных. Важную роль играет формирование и развитие корпоративной культуры кибербезопасности. Обучение работников основам информационной безопасности, проведение регулярных тренингов, разработка внутренних регламентов и инструкций по защите данных, а также формирование осознания ответственности за сохранность информации – все это способствует снижению вероятности человеческого фактора как одной из главных причин утечек данных.

Кроме того, особое внимание следует уделять вопросам управления рисками, связанными с обработкой персональных данных. Разработка и внедрение программ управления информационными рисками, проведение регулярных аудитов безопасности, анализ инцидентов и постоянное совершенствование системы защиты данных позволяют компаниям своевременно выявлять уязвимости и принимать меры по их устранению.

Только комплексный подход, включающий правовые, организационные и технические меры, может гарантировать эффективную защиту персональной информации работников. Внедрение современных технологий, соблюдение законодательных требований, развитие культуры информационной безопасности и постоянный мониторинг рисков создадут надежную систему защиты персональных данных. Это, в свою очередь, будет способствовать не только снижению угроз и предотвращению утечек информации, но и укреплению доверия работников, партнеров и клиентов к компании. Доверие является важнейшим активом любой организации, а обеспечение безопасности персональных данных становится неотъемлемым элементом успешной и устойчивой бизнес-стратегии.

Библиография

1. Дорджиева Н. Г. Анализ современного состояния проблемы защиты персональных данных работников предприятия // E-Scio. 2023. № 4(79). С. 21-25.
2. Мунтян С. И. Защита прав работника в судебном порядке при разглашении

работодателем персональных данных // Научное обеспечение агропромышленного комплекса: Сборник статей по материалам 79-й научно-практической конференции студентов по итогам НИР за 2023 год. В 2-х частях, Краснодар, 25 апреля 2024 года. Краснодар: Кубанский государственный аграрный университет им. И.Т. Трубилина, 2024. С. 923-925.

3. Куемжиева Я. Н. Роль судебной практики в формировании и реализации принципов гражданского судопроизводства // Тенденции развития науки и образования. 2023. № 103. С. 98-100. DOI: 10.18411/trnio-11-2023-217.

4. Карташова Д. А. Защита персональных данных работника // Студенческий. 2018. № 11-7(31). С. 33-36.

5. Латыпова Д. Р. Проблемы защиты персональных данных работника // LXX молодёжная научная конференция, посвящённая 75-й годовщине Победы в Великой Отечественной войне и 100-летию со дня рождения В. П. Лукачёва: тезисы докладов, Самара, 20-22 мая 2020 года. Самара: Самарский национальный исследовательский университет имени академика С.П. Королева, 2020. С. 170-171.

6. Рымашевская Д. Защита персональных данных работника в России и в Польше // Современные проблемы юридической науки: Материалы XVI Международной научно-практической конференции молодых исследователей, Челябинск, 24-25 апреля 2020 года / Министерство науки и высшего образования Российской Федерации Южно-Уральский государственный университет Юридический институт. Том Часть II. Челябинск: Издательский центр ЮУрГУ, 2020. С. 149-151.

7. Бычкова О. В. Защита персональных данных наемных работников // Актуальные проблемы государственного и муниципального управления: теоретико-методологические и прикладные аспекты: Материалы Всероссийского научно-практического круглого стола, Донецк, 21 мая 2024 года. Донецк: Донецкий государственный университет, 2024. С. 16-18.

8. Крыщенко Н. И. Разработка схемы и определение методов защиты персональных данных работников и клиентов на малом предприятии // Молодежная научная школа кафедры "Защищенные системы связи". 2020. Т. 1, № 2(2). С. 69-71.

9. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. 2020. № 1. С. 29-33.

10. Майстренко Г. А. Источники правового регулирования защиты персональных данных работника в России // Legal Bulletin. 2021. Т. 5, № 1. С. 24-29.

11. Афанасьев И. В. Правовые основы профессиональной деятельности. М.: Издательство Юрайт, 2019. 155 с.

12. Уварова Ю. А. Юридические гарантии защиты персональных данных работника в трудовом законодательстве РФ // Молодой ученый. 2018. № 19(205). С. 328-330.

13. Веред Е. Б. Об усилении уголовно-правовой защиты персональных данных работника // Вопросы трудового права. 2021. № 8. С. 588-595. DOI: 10.33920/pol-2-2108-03.

14. Коробкова О. К. Проблемные вопросы информационной безопасности организаций в рамках экономической безопасности РФ // Вестник Хабаровского государственного университета экономики и права. 2021. № 1 (105). С. 48-54.

15. Попова С. А., Соловьев М. А. Защита персональных данных работников // Вестник магистратуры. 2018. № 12-5 (87).

16. Абабкова А. Ю. Защита персональных данных медицинских работников: проблемы теории и практики // Медицинское право: новые правовые вызовы в работе медицинских организаций: Материалы IV Международного форума по медицинскому праву, Екатеринбург, 25-26 апреля 2024 года. Екатеринбург: Уральский государственный

юридический университет им. В.Ф. Яковлева, 2024. С. 155-160.
17. Гаджиев Х. И. Защита частной жизни в цифровую эпоху // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 6. С. 5-20. DOI: 10.12737/jflcl.2019.6.1.
18. Карпова Е. В. Защита персональных данных работников // Актуальные вопросы теории и практики финансово-хозяйственной деятельности: Сборник материалов IV Всероссийской (национальной) научно-практической конференции, Воронеж, 30 марта 2022 года. Воронеж, 2022. С. 154-157.
19. Мусаева Г. Б. Защита персональных данных работников // Роль аграрной науки в устойчивом развитии сельских территорий: Сборник IX Всероссийской (национальной) научной конференции с международным участием, Новосибирск, 20 декабря 2024 года. Новосибирск: ИЦ НГАУ "Золотой колос", 2024. С. 1282-1285.
20. Соколова Ж. В. Особенности защиты персональных данных работников в общеобразовательных учреждениях Крыма // Проблемы информационной безопасности: V Всероссийская с международным участием научно-практическая конференция, Симферополь-Гурзуф, 14-16 февраля 2019 года / Крымский федеральный университет имени В.И. Вернадского. Симферополь-Гурзуф: ИП Зуева Т. В., 2019. С. 142-144.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье являются, как это следует из ее наименования, современные вызовы в обеспечении защиты персональных данных работников. Заявленные границы исследования соблюдены ученым.
Методология исследования в тексте статьи не раскрывается.
Актуальность избранной автором темы исследования несомненна и обосновывается им следующим образом: "В условиях стремительного развития информационных технологий, глобальной цифровизации и широкомасштабного внедрения электронных систем хранения и обработки данных вопросы защиты персональных данных приобретают особую значимость. Современное общество, основанное на принципах технологической взаимосвязанности и оперативного обмена информацией, сталкивается с растущими рисками несанкционированного доступа к конфиденциальной информации, неправомерного использования персональных данных, их утечки, модификации и уничтожения вследствие кибератак, технических сбоев или действий третьих лиц. Эти угрозы затрагивают как физических лиц, так и юридических субъектов, ведущих деятельность в различных сферах экономики и общественных отношений. В особенности указанная проблема касается персональных данных работников, обрабатываемых работодателями в ходе исполнения трудовых отношений и кадрового администрирования. Такие данные включают сведения о личности работников, их профессиональной деятельности, медицинских показателях, финансовом положении и иных аспектах, что делает их объектами повышенного внимания со стороны злоумышленников и требует надежной правовой и технической защиты на всех этапах их жизненного цикла". Дополнительно ученому необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, а также раскрыть степень их изученности.
Научная новизна работы проявляется в ряде заключений автора: "Таким образом, защита персональных данных в условиях цифровой трансформации требует комплексного подхода, включающего как технические, так и организационные меры.

Внедрение надежных систем безопасности, использование современных технологий защиты, а также повышение уровня киберосведомленности персонала являются ключевыми факторами в обеспечении информационной безопасности. При этом соблюдение норм действующего законодательства, таких как Федеральный закон «О персональных данных», является обязательным требованием для всех организаций, работающих с персональными данными. В будущем можно ожидать ужесточения регулирования в данной сфере, что потребует от компаний дополнительных инвестиций в информационную безопасность и внедрения новых технологий защиты данных"; "... эффективная защита персональных данных требует комплексного подхода, включающего не только выполнение законодательных норм, но и внедрение современных технологий защиты информации, повышение уровня правовой грамотности работников и создание культуры осознания важности защиты данных в корпоративной среде. Соблюдение этих принципов позволит минимизировать риски нарушения законодательства, избежать значительных штрафов и обеспечить надежную защиту персональных данных работников и клиентов компании"; "Защита персональных данных работников является многогранной и комплексной задачей, требующей скоординированных действий в технологической, правовой и организационной сферах. В условиях стремительного развития цифровых технологий и процессов цифровой трансформации бизнеса компании сталкиваются с растущими вызовами, связанными с обеспечением информационной безопасности. Угрозы, такие как утечки конфиденциальной информации, несанкционированный доступ, кибератаки, вредоносное программное обеспечение и социальная инженерия, становятся все более распространенными и сложными. Одним из ключевых аспектов защиты персональных данных является совершенствование нормативно-правового регулирования, устанавливающего требования к обработке, хранению и передаче информации. В современных условиях необходимо учитывать, как национальное законодательство, так и международные стандарты в области защиты данных, такие как Общий регламент по защите данных (GDPR), Конвенция 108+ Совета Европы и другие нормативные акты. Внедрение строгих стандартов безопасности позволяет повысить уровень правовой защиты работников и снизить вероятность нарушений, связанных с обработкой их персональных данных" и др. Таким образом, статья вносит определенный вклад в развитие отечественной правовой науки и, безусловно, заслуживает внимания потенциальных читателей.

Научный стиль исследования выдержан автором в полной мере.

Структура работы логична. Во вводной части статьи ученый обосновывает актуальность избранной им темы исследования. Основная часть статьи состоит из двух разделов: "Современные вызовы и технологические риски в области защиты персональных данных"; "Правовое регулирование и организационные меры защиты персональных данных". В заключительной части работы содержатся выводы по результатам проведенного исследования.

Содержание статьи соответствует ее наименованию и не вызывает особых нареканий.

Библиография исследования представлена 20 источниками (научными статьями). С формальной точки зрения этого достаточно.

Апелляция к оппонентам имеется, но носит общий характер. В научную дискуссию с конкретными учеными автор не вступает, ссылаясь на ряд теоретических источников исключительно в обоснование своих суждений либо для иллюстрирования отдельных положений работы.

Выводы по результатам проведенного исследования имеются ("Защита персональных данных работников является многогранной и комплексной задачей, требующей скоординированных действий в технологической, правовой и организационной сферах.

В условиях стремительного развития цифровых технологий и процессов цифровой трансформации бизнеса компании сталкиваются с растущими вызовами, связанными с обеспечением информационной безопасности. Угрозы, такие как утечки конфиденциальной информации, несанкционированный доступ, кибератаки, вредоносное программное обеспечение и социальная инженерия, становятся все более распространенными и сложными. Одним из ключевых аспектов защиты персональных данных является совершенствование нормативно-правового регулирования, устанавливающего требования к обработке, хранению и передаче информации. В современных условиях необходимо учитывать, как национальное законодательство, так и международные стандарты в области защиты данных, такие как Общий регламент по защите данных (GDPR), Конвенция 108+ Совета Европы и другие нормативные акты. Внедрение строгих стандартов безопасности позволяет повысить уровень правовой защиты работников и снизить вероятность нарушений, связанных с обработкой их персональных данных. Не менее важным направлением является использование современных технологических решений, обеспечивающих высокий уровень защиты информации. Среди таких решений можно выделить системы шифрования данных, средства контроля доступа, биометрическую аутентификацию, инструменты мониторинга активности пользователей, системы предотвращения утечек данных (DLP) и средства защиты от вредоносных программ. Применение передовых технологий способствует минимизации рисков несанкционированного распространения персональной информации и повышает общий уровень кибербезопасности в организации. Однако технологические меры сами по себе не могут гарантировать абсолютную защиту персональных данных. Важную роль играет формирование и развитие корпоративной культуры кибербезопасности. Обучение работников основам информационной безопасности, проведение регулярных тренингов, разработка внутренних регламентов и инструкций по защите данных, а также формирование осознания ответственности за сохранность информации – все это способствует снижению вероятности человеческого фактора как одной из главных причин утечек данных"), обладают свойствами достоверности, обоснованности и, несомненно, заслуживают внимания научного сообщества.
Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере административного права, информационного права при условии ее доработки: раскрытии методологии исследования, дополнительном обосновании актуальности его темы (в рамках сделанного замечания), введении дополнительных элементов дискуссионности.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ
на статью на тему «Современные вызовы в обеспечении защиты персональных данных работников».

Предмет исследования.
Предложенная на рецензирование статья посвящена актуальным вопросам обеспечения защиты персональных данных работников. Автором сделан акцент на гражданско-правовых механизмах охраны персональных данных на современном этапе развития общества, когда персональные данные активно используются в различных целях, в том числе в цифровом пространстве. Раскрываются проблемы современных вызовов и

технологических рисков в области защиты персональных данных, правовое регулирование и организационные меры защиты персональных данных. Предлагается раскрытие заявленных проблема с точки зрения «комплексного подхода, включающего не только выполнение законодательных норм, но и внедрение современных технологий защиты информации, повышение уровня правовой грамотности работников и создание культуры осознания важности защиты данных в корпоративной среде». В качестве конкретного предмета исследования выступили, материалы практики, положения нормативно-правовых актов, мнения ученых по тематики защиты персональных данных.

Методология исследования.

Цель исследования прямо в статье не заявлена. При этом она может быть ясно понята из названия и содержания работы. Цель может быть обозначена в качестве рассмотрения и разрешения отдельных проблемных аспектов вопроса об обеспечении защиты персональных данных работников. Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования. Как указано в самой статье, «Методология исследования строится на комплексном подходе, объединяющем анализ нормативно-правовой базы и экспертные оценки. Такой подход обусловлен необходимостью всестороннего изучения проблемы, учитывая как юридические аспекты, так и практические реалии функционирования систем обработки персональных данных в организациях».

В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из материалов практики.

Наибольшую роль сыграли специально-юридические методы. В частности, автором активно применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства, посвященного защите персональных данных. Например, следующий вывод автора: «В Российской Федерации основным нормативно-правовым актом, регулирующим отношения в данной сфере, является Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», который определяет основные принципы, правовые основания и требования к обработке, хранению, передаче и уничтожению персональных данных. Данный закон закрепляет права субъектов персональных данных, устанавливает обязанности операторов по их обработке, предусматривает меры защиты информации и ответственность за допущенные правонарушения». В целом по статье приводятся авторские подходы к тому, как следует толковать положения действующего законодательства применительно к персональным данным и их защите.

Следует положительно оценить возможности эмпирического метода исследования. Автором делаются выводы по поводу того, как совершенствовать режим охраны персональных данных с учетом статистики и иных данных. Например, указано, что «в 2023 году Роскомнадзор оштрафовал ряд крупных российских компаний за несоблюдение требований о хранении и обработке персональных данных, поскольку в их внутренних политиках отсутствовали положения о порядке удаления информации по истечении сроков хранения».

Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.

Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема обеспечения защиты персональных данных работников сложна и неоднозначна. В настоящий момент, когда с развитием сети интернет, а также форм и

механизмов хакерской деятельности увеличилось число и объем утечек персональных данных, важным является обеспечение сохранности персональных данных работников. Массовые утечки персональных данных могут иметь неблагоприятные последствия, прежде всего, в плане потенциальной угрозы правам и законным интересам граждан. Сложно спорить с автором в том, что «угрозы затрагивают как физических лиц, так и юридических субъектов, ведущих деятельность в различных сферах экономики и общественных отношений. В особенности указанная проблема касается персональных данных работников, обрабатываемых работодателями в ходе исполнения трудовых отношений и кадрового администрирования. Такие данные включают сведения о личности работников, их профессиональной деятельности, медицинских показателях, финансовом положении и иных аспектах, что делает их объектами повышенного внимания со стороны злоумышленников и требует надежной правовой и технической защиты на всех этапах их жизненного цикла». Приводимые автором в статье примеры из практики наглядно демонстрирует этот вопрос.

Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.

Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:

«Только комплексный подход, включающий правовые, организационные и технические меры, может гарантировать эффективную защиту персональной информации работников. Внедрение современных технологий, соблюдение законодательных требований, развитие культуры информационной безопасности и постоянный мониторинг рисков создадут надежную систему защиты персональных данных. Это, в свою очередь, будет способствовать не только снижению угроз и предотвращению утечек информации, но и укреплению доверия работников, партнеров и клиентов к компании».

Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.

Во-вторых, автором предложены идеи по совершенствованию действующего законодательства. В частности,

«Одним из ключевых аспектов защиты персональных данных является совершенствование нормативно-правового регулирования, устанавливающего требования к обработке, хранению и передаче информации. В современных условиях необходимо учитывать, как национальное законодательство, так и международные стандарты в области защиты данных, такие как Общий регламент по защите данных (GDPR), Конвенция 108+ Совета Европы и другие нормативные акты».

Приведенный вывод может быть актуален и полезен для правотворческой деятельности.

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «Юридические исследования», так как она посвящена правовым проблемам, связанным с защитой персональных данных работников на современном этапе.

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел проблемы, выявил наиболее важные вопросы защиты персональных данных работников, в частности, в плане потенциальных утечек баз данных. В полной мере можно считать достигнутой цель исследования, так как автор предложил некоторые решения проблемы защиты персональных данных работников как юридического, так и технического плана.

Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.

Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.
Библиография.
Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России (Дорджиева Н.Г., Мунтян С.И., Афанасьев И.В., Попова С. А., Соловьев М. А. и другие). Многие из цитируемых ученых являются признанными учеными в области защиты персональных данных.
Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.
Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.
Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к проблемы создания юридической и технической базы эффективной защиты персональных данных работников.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи
«Рекомендую опубликовать»